

566030 -- Patent Information

Published Serial No.	5 6 6 0 3 0								
Title	Wireless LAN authentication method								
Patent type	B								
Date of Grant	2003/12/11								
Application Number	091115103								
Filing Date	2002/7/8								
IPC	H04L9/00								
Inventor	WANG, HSIAO-HUNG(TW)								
Applicant	<table border="1"><tr><th>Name</th><th>Country</th><th>Individual/Company</th></tr><tr><td>QUANTA COMPUTER INC.</td><td>TW</td><td>Company</td></tr></table>			Name	Country	Individual/Company	QUANTA COMPUTER INC.	TW	Company
Name	Country	Individual/Company							
QUANTA COMPUTER INC.	TW	Company							
Abstract	<p>The present invention provides an authentication method applied in a Wireless LAN. In accordance with the present invention, it is not necessary to register the ISP before use. In other words, when the user suddenly needs to check the network information, the user may transmit the identification data and the requiring online service time to the server through the safety online state that is built in real time. At the same time, the server may receive the fee according to the online server time.</p>								

Available features	
<input type="checkbox"/> 1 / 1 FAMPAT - Patent Families - ?	
QUESTEL-ORBIT	
TW-566030 Wireless local area network authentication method	
Family/Accession Nbr	20042802424957
Patent Number	TW566030 B 20031211 [TW-566030] <input checked="" type="checkbox"/> US2004004958 A1 20040108 [US20040004958]
Title	Wireless local area network authentication method
Patent Assignee	QUANTA COMP INC
Orig. Patent Assignee	QUANTA COMPUTER INC. (TW)
Inventor(s)	WANG HSIAO-HUNG
Application Nbr	2002TW-0115103 20020708 2002US-0265541 20021003
Priority Details	2002TW-0115103 20020708
IPC	H04L-009/00 H04L-012/14 H04L-012/28 H04L-012/56 H04L-012/66 H04L-029/06 H04M-017/00 H04Q-007/24
IPC Advanced All	H04L-012/14 [2006-01 A - I R M EP] H04L-012/28 [2006-01 A - I R M EP] H04L-012/56 [2006-01 A - I R M EP] H04L-029/06 [2006-01 A - I R M EP] H04M-017/00 [2006-01 A - I R M EP]
IPC Core All	H04L-012/14 [2006 C - I R M EP] H04L-012/28 [2006 C - I R M EP] H04L-012/56 [2006 C - I R M EP] H04L-029/06 [2006 C - I R M EP] H04M-017/00 [2006 C - I R M EP]
ECLA	H04L-012/14 H04L-012/28P1 H04L-012/28W H04L-012/56B H04L-029/06S8 H04M-017/00 H04W-006/06
ICO Code	T04M-215/20D T04M-215/22 T04M-215/32 T04W-002/16 T04W-023/06 T04W-050/065
US Class	ORIGINAL (O) : 370352000; CROSS-REFERENCE (X) : 370338000
Abstract	(US20040004958) The present invention describes an authentication method applied in a Wireless LAN. In accordance with the present invention, it is not necessary for the user to register on the Internet supply provider (ISP) before using. In other words, when the user is in urgent need of checking network information, the user transmits the identification data and the required connection time to the account server through the safe physical connection line between the user and the account server. At the same time, the server receives the fee according to the connection time.
Object of Invention	(US20040004958) The present invention describes an authentication method applied in a Wireless LAN. The main purpose of this authentication method is to accelerate the communication process between the user and the server. The main purpose of this challenge text is to check whether the shared key held by

	the user is same as that held by the access point.
Advantages / Prev. Drawbacks	(US20040004958) First, the user needs to build a safe physical connection line between the user and the account server. For example, it is difficult to require the users to keep the secret of the shared key in the Wireless LAN access point authentication. On the other hand, the main drawback existing in the outside account server authentication is that the user must register on the account server first. This is very inconvenient for users who are in urgent need.
Independent Claims	(US20040004958) 1. An authentication method applied in a Wireless Local Area Network (WLAN), comprising: providing a server and a client; building a safe connection line between said server and said client; prepaying a connection fee to said server by said client according to a predetermined connection time of said client; sending a question regarding identification data of said client from said server through said safe connection line after said server receives said connection fee; responding to said question by said client through said safe connection line; and connecting an Internet from said client through said Wireless LAN after said server confirms said connection requirement. 10. An authentication system applied in a Wireless LAN, comprising: a server for account management; a client prepaying a connection fee to said server according to a predetermined connection time of said client; a safe connection line existing between said client and said server, wherein said server asks said client for an identification data through said safe connection line and said client responds and sends a connection requirement to said server through said safe connection line; and a gateway controlling the connection line between said client and said server according to an account management record stored in said server.
Update New docs	2004-27

公告本

申請日期	91.7.8.
案號	91115103
類別	H04L 9/00

(以上各欄由本局填註)

A4

C4

566030

發明專利說明書
新型

一、發明 新 型 名稱	中文	無線區域網路認證方法
	英文	Wireless LAN Authentication Method
二、發明人 創 人	姓名	王孝弘 WANG, Hsiao-Hung
	國籍	中華民國
	住、居所	台北市和平西路一段 170 號 12 樓之 3 12F-3, No 170, Sec 1, Ho Ping W Rd, Taipei City, TAIWAN, R.O.C
三、申請人	姓名 (名稱)	廣達電腦股份有限公司 QUANTA COMPUTER INC.
	國籍	中華民國
	住、居所 (事務所)	桃園縣龜山鄉文化二路 188 號 NO.188, WEN HWA 2 ND RD., KUEI SHAN HSIANG, TAOYUAN HSIEN, TAIWAN, R.O.C.
代表人 姓名	林百里 LAM, Barry	

裝訂線

四、中文發明摘要(發明之名稱)

(請先閱讀背面之重要事項再填寫各欄)

裝

訂

線

無線區域網路認證方法

本發明提供一種帳號伺服器認證方法，具備有獨立收費的功能，使用者不需事先向任何之網際網路服務提供者進行註冊，當使用者突發性的需要使用網路資源時，使用者端可將其識別資料和欲使用之連線時間透過即時建立之安全性之連線傳送至帳號伺服器獲得連線，同時伺服器端亦可透過所使用之連線時間進行對價之收費。

英文發明摘要(Wireless LAN Authentication Method)

The present invention provides an authentication method applied in a Wireless LAN. In accordance with the present invention, it is not necessary to register the ISP before use. In other words, when the user suddenly needs to check the network information, the user may transmit the identification data and the requiring online service time to the server through the safety online state that is built in real time. At the same time, the server may receive the fee according to the online server time.

五、發明說明()

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

發明領域：

本發明係有關於一種認證方法，特別是有關於一種使用在無線區域網路上之認證方法，具備有獨立收費的功能，能讓無線區域網路服務之提供者能主動管制無線區域網路之使用者，且讓無線區域網路之使用者能就無線區域網路服務之提供者之所在即時使用服務而不必事先成為骨幹網路之用戶。

發明背景：

由於可攜式電腦和掌上型電腦普及率之快速成長，無線區域網路對今日的電腦及通訊工業來講，將成為一項重要的觀念及技術。在無線區域網路架構中，電腦主機不需要像在傳統之有線網路裡，必須保持固定在網路架構中之某個節點上，而是可以在任易之時間做任何之移動，也能對網路之資料作任意之擷取。

有兩種不同類型之無線區域網路基本架構，第一種為有基礎架構之無線區域網路 (Infrastructure Wireless LAN)，所謂基礎架構就是一個現存之有線網路分散式系統，請參閱第一 A 圖所示，筆記型 (notebook) 電腦 100 以無線

五、發明說明()

電的方式傳送訊號到天線 101，然後經由天線 101 將接收到的訊號送至傳送器(transmitter)102，以降低所接收到的訊號之頻率並傳送到橋接器 103 (access point)。然後橋接器 103，將所收到的訊號傳送到區域網路 104。其傳送的方法是以有線傳送的方式，透過電纜線 105 將訊號傳送到區域網路 104 上，所以筆記型(notebook)電腦 100 透過電纜線 105 可以連線到區域網路 104。

另一種無線區域網路基本架構為無基礎架構之無線區域網路(Ad Hoc Wireless LAN)，為用戶端與用戶端間之直接互連，如第一 B 圖所示，由橋接器 115 (Access Point) 接收到個人電腦 100 所傳送的資料框，並透過區域網路 107 的閘道器 106(gateway)送到網際網路 109。並依據資料框上的目的地主機網際網路協定層位址(IP address)，此資料框會到達位於區域網路 114 的閘道器 112。然後橋接器 160 將所接收到的資料再以無線的方式，傳送到個人電腦 128。所以這兩部個人電腦便可以用來互相傳遞資料，例如網路電話(Internet phone)、視訊會議(video conference)或遠距教學等，都可以利用此無線網路結構來進行。

為管制資料之保密性，通常於進行資料傳輸前會有一認證(Authentication)工作，認證之目的是確認對方身份之合法性，以免與身份不明之對象溝通，洩漏了重要

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明()

(請先閱讀背面之注意事項再填寫本頁)

裝
訂

機密，亦即雙方進行通訊前需經過認證。一般認證方法分為無線區域網路橋接器認證和外部帳號伺服器認證兩種類型，其中無線區域網路橋接器認證又分為開放系統式(Open system)與共享密匙式(Shared Key)兩種。

開放系統式認證實際上即是一種不需認證演算之認證方法，這種方式主要是讓工作站簡單表明身份，以便雙方可儘速進行通訊。而共享密匙式認證是一種加密解密方法，其特點為認證雙方允許擁有共同之密碼，即 Shared Key，擁有密碼之用戶端於欲透過無線網路橋接器連接網路前，需先向無線網路橋接器發出建立連線請求。接獲連線請求之無線區域網路橋接器會回應發出請求之用戶端一盤問全文(Challenge Text)，並將其送至用戶端，讓用戶端利用密匙將盤問全文加密並回傳，此全文之目的是要求檢驗對方之密匙。接著此無線網路橋接器會將收到之盤問全文用其擁有之密匙解密。若所解出之盤問全文與當初送出者相同，則表示用戶端擁有相同之密匙，則用戶端即可透過無線區域網路橋接器連線網路。

外部帳號伺服器認證，係另外建置一專責認證用戶端使用權之帳號伺服器，用戶端於帳號伺服器登記有帳號及密碼資料。使用外部帳號伺服器時，會先開放所有用戶端連線網路，在用戶端通過認證前僅能先連線外部帳號伺



五、發明說明()

服務器，待用戶端通過帳號伺服器認證後，始能經由閘道器連線網際網路。

傳統上此兩種認證方法均有其缺點存在，對於無線區域網路橋接器認證方式，其很難要求具有共享密匙之用戶端不洩漏此共享密匙予未經許可之用戶端，使得網路資源讓無許可之用戶端無償使用。而外部帳號伺服器認證方式，其缺點為用戶端需先註冊於外部帳號伺服器，並取得外部帳號伺服器所指定之帳號與密碼後，使用此帳號與密碼方能通過認證使用網路資源，其對於急需使用網路資源之用戶端而言常常緩不濟急。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

發明目的及概述：

鑑於上述所提出之習知無線區域網路橋接器認證和外部帳號伺服器認證兩種方法皆有其缺點存在。

因此，本發明提出一種網路認證方法，其利用一具獨立收費功能之帳號伺服器，當用戶端欲透過帳號伺服器之認證以進行連線時，首先於用戶端使用者與伺服器建立具備安全性之實體連線。接著用戶端根據所預定使用無線區域網路之時間長短，向帳號伺服器繳付所需之費用。當帳號伺服器接收到用戶端之連線費用後，會透過先前所述

五、發明說明()

(請先閱請背面之注意事項再填寫本頁)

裝
訂

立之實體連線向用戶端詢問其識別資料。此時用戶端透過具安全性之實體連線，對帳號伺服器所詢問之資料做出回應，並送出連線請求。接著帳號伺服器會回覆用戶端之連線請求。此時用戶端即可透過無線區域網路界面連線至網際網路，並可連至其他網站。

本發明之帳號伺服器具備有下述功能，其具有一個不被第三人窺探之通訊界面，因此欲使用網路連線之用戶端，可透過此界面將識別資料傳送與伺服器，同時根據所欲使用之網路連線時間繳交對應之預付費用給伺服器，此時伺服器會通知閘道器給予用戶端連線，並根據用戶端之預付費用來控制用戶端之連線時間，因此本發明之伺服器具備有獨立收費之功能，且能根據用戶端之預付費用來控制用戶端之連線時間。因此，藉由本發明之無線網路認證方法，不僅能讓突發性的需要使用網路資源之使用者，只要再具備無線網路服務涵蓋之範圍內，不需事先透過繁複之註冊程序，隨時可透過無線網路連線，且對無線網路服務提供者而言，能過濾掉於傳統技藝中可能多能共享一網路帳號，而造成無常使用網路資源之狀況發生。

圖式簡單說明：



五、發明說明()

為讓本發明之上述和其他目的、特徵、和優點能更明顯易懂，下文特舉一較佳實施例，並配合所附圖式，作詳細說明如下

第一 A 圖所示為傳統有基礎架構之無線區域網路結構圖：

第一 B 圖所示為傳統的無基礎架構之無線區域網路 (Ad Hoc Wireless LAN) 結構圖；

第二圖所示為外部帳號伺服器認證方式，其外部帳號伺服器係放置於入口網站中；

第三圖所示為外部帳號伺服器認證方式，其外部帳號伺服器係放置於網際網路服務提供者 (ISP) 處；

第四圖所示為本發明的無線區域網路伺服器認證方法結構圖；以及

第五圖所示為本發明的無線區域網路伺服器認證方法流程圖。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

絲

圖號對照說明：

100 筆記型電腦

101 天線

102 傳送器

103 橋接器

104 區域網路

105 電纜線

五、發明說明()

- | | |
|--------------|-------------|
| 106 閘道器 | 107 區域網路 |
| 109 網際網路的 | 112 閘道器 |
| 114 區域網路 | 115、160 橋接器 |
| 128 個人電腦 | 10 無線區域網路 |
| 12 伺服器 | 14 網際網路 |
| 16 其他網站 | 18 用戶端 |
| 20 無線區域網路橋接器 | |

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

在不限制本發明之精神及應用範圍之下，以下即以一實施例，介紹本發明之實施；熟悉此領域技藝者，在瞭解本發明之精神後，當可應用此方法於各種不同之無線網路認證過程中。藉由使用本發明之認證方法，不僅可管制無線網路使用者，且可讓使用者根據自己預定使用之總時數繳交使用費用，隨時連線無線網路，而不需如傳統般繳交月費。且根據本發明之方法，無線網路之提供者，能記錄使用者所使用之時間，根據使用者登錄要求之使用時間來控制無線網路資源之提供，且能讓使用者在無線網路服務之範圍內，隨時登錄使用對價之網路資源。且本發明之認證方法並不像傳統技藝般，在登錄使用無線網路資源時，

五、發明說明()

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
綫

需先註冊於外部帳號伺服器，並取得外部帳號伺服器所指定之帳號與密碼後，使用此帳號與密碼方能通過認證使用網路資源，如此認證之方式，往往需耗費數個工作天，對於一個突發性的要求使用網路資源之使用者來說，往往緩不濟急，且對於無線區域網路服務提供者來說，亦會喪失部分商機，因此本發明提供一種全新之認證方法，能解決上述之全部問題，達到雙贏之目的。本發明之應用當不僅限於以下所述之實施例。

為了使無線區域網路之使用者能達到即時認證使用網路資源資源之目的，且無線區域網路之服務提供者，能同時達到管制之目的，不使無線網路資源讓無許可之用戶端無償使用，所以本發明提供了一個無線網路的認證方法，使得無線網路之提供者，能記錄使用者所使用之時間，根據使用者登錄要求之使用時間來控制無線網路資源之提供，且能讓使用者在無線網路服務之範圍內，隨時登錄使用對價之網路資源。

傳統之外部帳號伺服器認證方式如第二圖與第三圖所示。其中以第二圖為例，其外部帳號伺服器係放置於入口網站中，當用戶端靠近無線區域網路閘道器時，即可透過瀏覽器連至入口網站帳號伺服器進行登錄如虛線 1 所示，接著如虛線 2，帳號伺服器會檢核該登錄之帳號與密



五、發明說明()

(請先閱讀背面之注意事項再填寫本頁)

碼，若為會員之帳號與密碼，則核准該用戶端連上網路，進入其他網站如虛線 3。而第三圖所示為傳統帳號伺服器之另一種認證方法，其外部帳號伺服器係放置於網際網路服務提供者（ISP）處由其所管理，此時當用戶端靠近無線區域網路閘道器時，即可透過瀏覽器連至網際網路服務提供者之帳號伺服器中進行登錄如虛線 1 所示，接著如虛線 2，帳號伺服器會檢核該登錄之帳號與密碼，若為會員之帳號與密碼，則核准該用戶端經由該網際網路服務提供者連上網路，進入其他網站如虛線 3。

然上述之認證方法，常發生無線網路資源讓無許可之用戶端無償使用，且傳統之申請帳號之方法往往需耗費很長之時間，造成不能讓使用者在無線網路服務之範圍內，隨著突發之需要而登錄使用。本發明的無線網路系統的結構如第四圖所示，其中無線區域網路 10、網際網路 14 和其他網站 16 的結構都和以往的無線網路系統一樣，所不同的是伺服器 12，其最大不同處在於，傳統上使用者端需先向網際網路服務提供者進行註冊之動作，並獲得指定之帳號與密碼後方能進行連線。然而，本發明提供一種新的帳號伺服器運作方法，不需事先向任何之網際網路服務提供者進行註冊，當使用者突發性的需要使用網路資源時，此時使用者端可將其識別資料透過即時建立之具備安全性之

裝

訂

線

五、發明說明()

(請先閱讀背面之注意事項再填寫本頁)

連線傳送，並獲得連線，因此本發明大大的提高了使用者的方便性。

請再次參閱第四圖，當用戶端 18 突發性的需要使用網路資源時，首先用戶端 18 之使用者需先與伺服器 12 建立具備安全性之實體連線，其方法可使用紅外線線傳輸或通用序列埠等，而用戶端 18 可為一膝上型 (laptop) 或筆記型 (notebook) 電腦、手持式裝置 (handheld device) 個人數位助理 (personal digital assistance, PDA) 等。當用戶端 18 與伺服器 12 建立具備安全性之實體連線後，用戶端 18 先向伺服器 12 端，根據所預定使用無線區域網路 10 之時間長短繳付所需之費用。當伺服器 12 端，接收到用戶端 18 所預繳之連線費用後，會透過先前所建立之實體連線向用戶端 18 詢問其識別資料，而其中識別資料可包括用戶端之中央處理器序號 (CPU Serial Number) 及界面之媒體存取控制位址 (MAC Address)，其中所謂媒體存取控制位址，即為用戶端 18 之無線網路卡的硬體位址。此時用戶端 18 即可針對伺服器 12 所詢問之資料做出回應，並送出連線請求。當伺服器 12 端收到用戶端 18 之回應後，會回覆用戶端 18 之連線請求，並於伺服器 12 之內部產生一筆帳號記錄，其係用以記載用戶端 18 之識別資料、繳付之費用，及根據此繳付費用所允許之連線時間。當用戶端



五、發明說明()

(請先閱讀背面之注意事項再填寫本頁)

18 或得連線允許後，即可在用戶端 18 之預付連線時間內經由無線區域網路橋接器、閘道器連至無線區域網路 10，進入網際網路 14，而連至其他網站 16 讀取所需資料其中而伺服器 12 可在無線區域網路 10 內部以虛擬位址為用戶端 18 定位，對外將此虛擬位址對應到真實位址並與通訊埠配對。

請參閱第五圖，為本發明建立連線之認證方法主要流程圖，當用戶端 18 欲透過帳號伺服器 12 之認證以進行連線時，其主要流程如下所示，其中虛線分別代表認證流程之步驟與參與該步驟之元件。當用戶端 18 突發性的需要使用網路資源時，首先於步驟 1 用戶端 18 使用者與伺服器 12 建立具備安全性之實體連線。接著步驟 2，用戶端 18 需根據所預定使用無線區域網路 10 之時間長短，向伺服器 12 繳付所需之費用。步驟 3，當伺服器 12 接收到用戶端 18 之連線費用後，會透過先前所建立之實體連線向用戶端 18 詢問其識別資料。步驟 4，此時用戶端 18 透過具安全性之實體連線，對伺服器 12 所詢問之資料做出回應，並送出連線請求。步驟 5，伺服器 12 會回覆用戶端 18 之連線請求，例如自動產生一組 ID/Password，回傳給用戶端 18，回傳機制包括紅外線傳輸、USB、PS/2、COM port 等方式。步驟 6，用戶端 18 透過無線區域網路界面連線至網際網路 14，

裝

訂

綫

五、發明說明()

而可連至其他網站 16。

藉由上述描述，本發明提供一種新的帳號伺服器運作方法，不需事先向任何之網際網路服務提供者進行註冊，亦即不需事先成為此網際網路服務提供者之用戶，當使用者突發性的需要使用網路資源時，此時使用者端可將其識別資料透過即時建立之具備安全性之連線傳送，並獲得連線，因此本發明大大的提高了使用者的方便性。

其中上述伺服器 12 除了會於內部產生一筆帳號記錄，用以記載用戶端 18 之識別資料、繳付之費用，及根據此繳付費用所允許之連線時間外，其更能根據所記錄之資料，通知網路閘道器使用時間已超過之用戶端，用以終止該用戶端之連線使用，同時亦將提出請求連線並預付連線費用之用戶端通知網路閘道器，以開啟該用戶端之網路使用。其中上述閘道器功能，可根據伺服器 12 內部之帳號記錄所有之用戶端資訊，核准預繳費用尚未用完之用戶端傳送資料，而阻擋已過連線時間或未具識別資料之用戶端傳送資料。

綜合上述，本發明之伺服器具備有下述功能，其具有一個不被第三人窺探之通訊界面，因此欲使用網路連線之用戶端，可透過此界面將識別資料傳送與伺服器，同時根據所欲使用之網路連線時間繳交對應之預付費用給伺服

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
綫

五、發明說明()

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
綫

器，此時伺服器會通知閘道器給予用戶端連線，並根據用戶端之預付費用來控制用戶端之連線時間，因此本發明之伺服器具備有獨立收費之功能，且能根據用戶端之預付費用來控制用戶端之連線時間。因此，藉由本發明之無線網路認證方法，不僅能讓突發性的需要使用網路資源之使用者，只要再具備無線網路服務涵蓋之範圍內，不需事先透過繁複之註冊程序，隨時可透過無線網路連線，且對無線網路服務提供者而言，能過濾掉於傳統技藝中可能多能共享一網路帳號，而造成無常使用網路資源之狀況發生。

以上所述僅為本發明之較佳實施例而已，並非用以限定本發明之申請專利範圍；凡其它未脫離本發明所揭示之精神下所完成之等效改變或修飾，均應包含在下述之中請專利範圍內。

六、申請專利範圍

(請先閱讀背面之注意事項再填寫本表)

裝

訂

申請專利範圍：

1. 一種無線區域網路認證方法，該認證方法具有收費之功能，至少包含下列步驟：

提供一伺服器與一用戶端；

建立具備安全性之實體連線於該伺服器與該用戶端間；

該用戶端根據所預定使用之一無線區域網路之時間長短向該伺服器繳付費用；

接收到該用戶端之費用後，該伺服器透過該所建立之實體連線向該用戶端詢問其識別資料；

回應該伺服器所詢問之資料並送出連線請求，其中該用戶端所做之回應均係透過該所建立之安全性實體連線進行；

回覆該用戶端之連線請求，當該伺服器確認該連線請求後；以及

該用戶端透過該無線區域網路連線至一網際網路。

2. 如申請專利範圍第1項之方法，其中上述之用戶端係由膝上型(laptop)電腦、筆記型(notebook)電腦、



六、申請專利範圍

手持式裝置 (handheld device) 與個人數位助理 (personal digital assistance, PDA) 中選擇其一。

(請先閱請背面之注意事項再填寫本頁)

裝
訂
綫

3. 如申請專利範圍第 1 項之方法，其中上述之安全性實體連線方法係使用紅外線線傳輸。

4. 如申請專利範圍第 1 項之方法，其中上述之安全性實體連線方法係使用通用序列埠。

5. 如申請專利範圍第 1 項之方法，其中上述之當該伺服器確認該連線請求後會於伺服器之內部產生一筆帳號記錄，其係用以記載該用戶端之識別資料、繳付之費用，及根據此繳付費用所允許之連線時間。

6. 如申請專利範圍第 1 項之方法，其中上述之識別資料可包括該用戶端之中央處理器序號 (CPU Serial Number) 及界面之媒體存取控制位址 (MAC Address)。

7. 如申請專利範圍第 1 項之方法，其中上述之伺服器會於該用戶端所繳之連線費用時間內提供連線服務。

六、申請專利範圍

8. 如申請專利範圍第1項之方法，其中上述之伺服器會於當該用戶端所繳之連線費用時間到達時中止連線服務。

9. 如申請專利範圍第1項之方法，其中上述之回覆該用戶端之連線請求，當該伺服器確認該用戶端連線請求後，會控制閘道器讓該用戶端進行連線。

10. 一種無線區域網路認證系統，具有收費之功能，該系統至少包含：

一伺服器，該伺服器具有帳號管理功能；

一用戶端，該用戶端根據所預定使用之一無線區域網路之時間長短向該伺服器繳付費用；

一具備安全性之實體連線，建立於該用戶端與該伺服器間，其中該伺服器透過該實體連線向該用戶端詢問其識別資料，而該用戶端亦透過該實體連線回應該伺服器所詢問之識別資料並可送出連線請求；以及

一閘道器，根據該伺服器內之帳號管理控制用戶端之連線該無線區域網路。

11. 如申請專利範圍第10項之系統，其中上述之用

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

練

戶端係由膝上型 (laptop) 電腦、筆記型 (notebook) 電腦、手持式裝置 (handheld device) 與個人數位助理 (personal digital assistance, PDA) 中選擇其一。

12. 如申請專利範圍第 10 項之系統，其中上述之安全性實體連線係為紅外線傳輸。

13. 如申請專利範圍第 10 項之系統，其中上述之安全性實體連線係為通用序列埠。

14. 如申請專利範圍第 10 項之系統，其中上述之帳號管理功能會記載該用戶端之識別資料、繳付之費用，及根據繳付費用所允許之連線時間。

15. 如申請專利範圍第 10 項之系統，其中上述之識別資料可包括該用戶端之中央處理器序號 (CPU Serial Number) 及界面之媒體存取控制位址 (MAC Address)。

16. 如申請專利範圍第 9 項之系統，其中上述之伺服器會於該用戶端所繳之連線費用時間內提供連線服務。



六、申請專利範圍

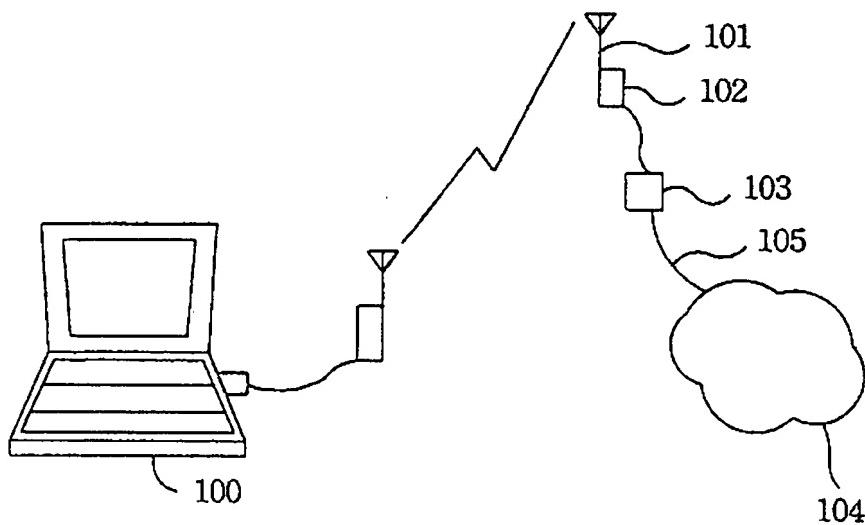
17. 如申請專利範圍第 10 項之系統，其中上述之伺服器會於當該用戶端所繳之連線費用時間到達時中止連線服務。

(請先閱讀背面之注意事項再填寫本頁)

裝
訂

線

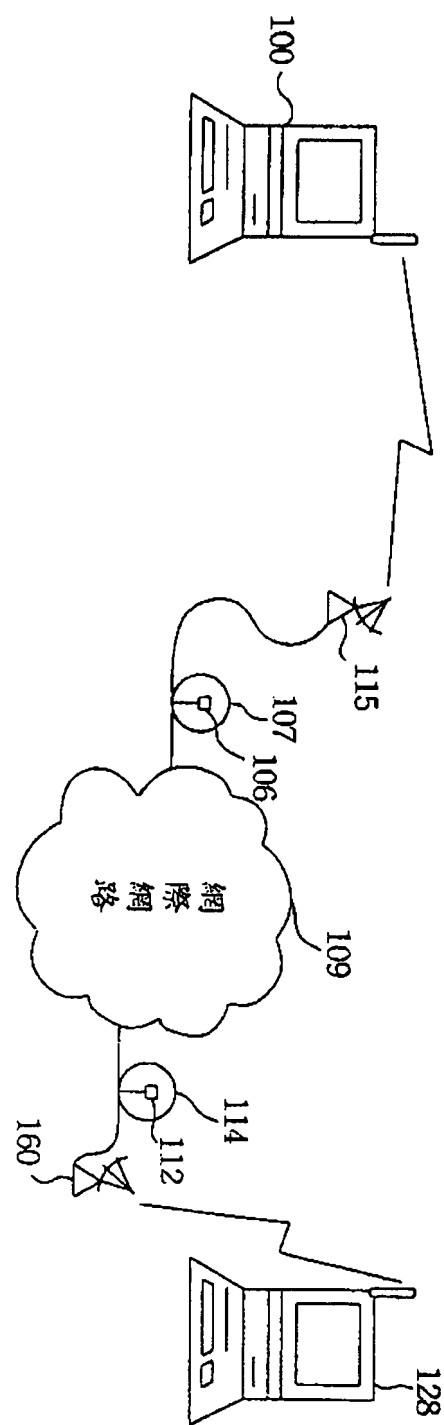




第一A圖

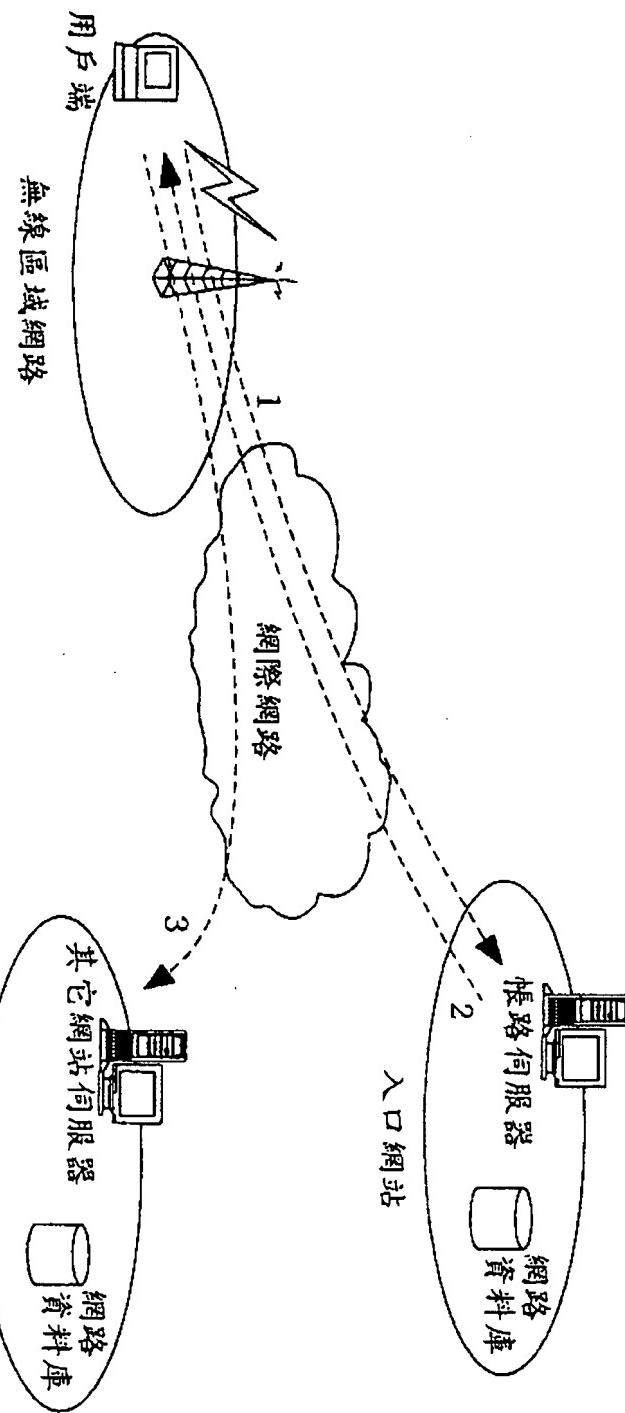
EDGEE

第一-B圖



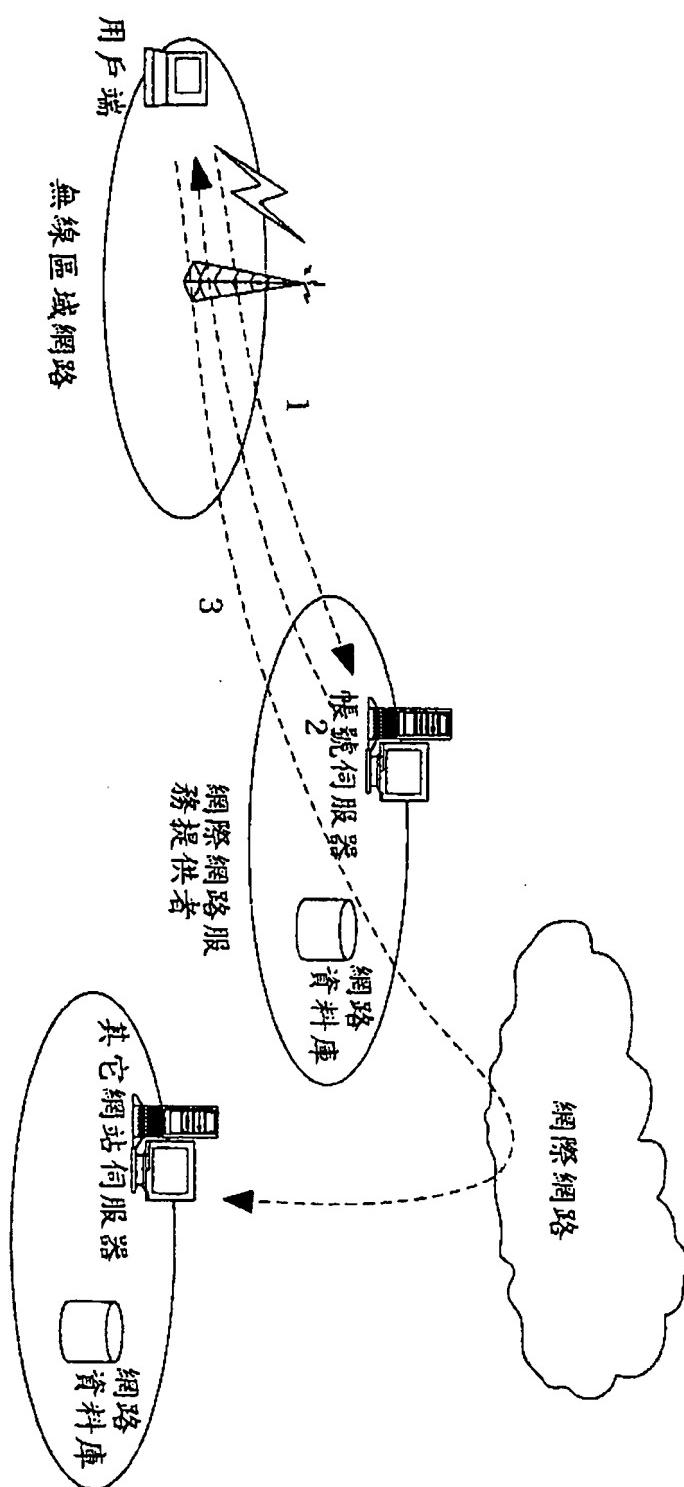
EDU

第二圖



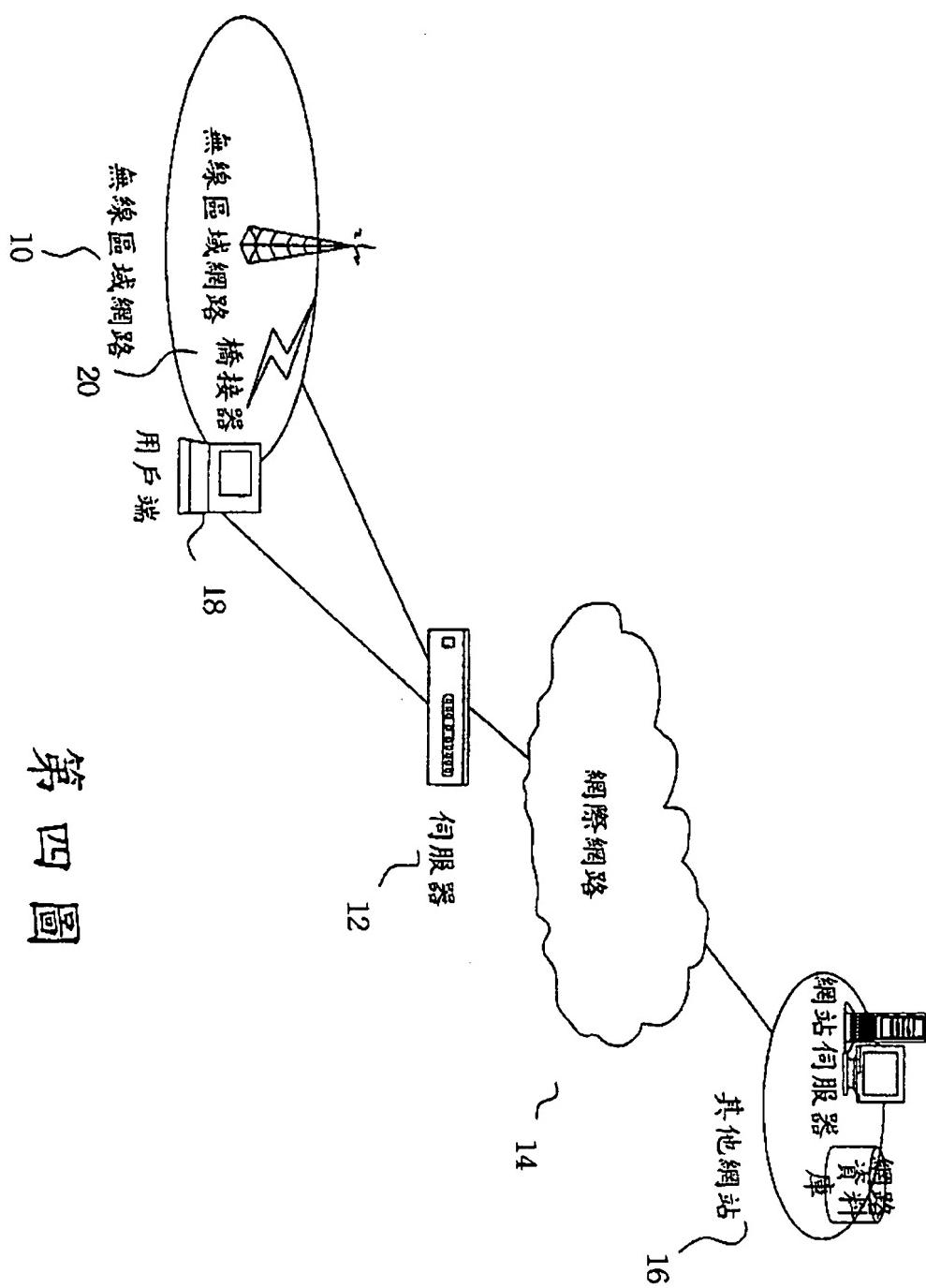
上
中
下

FREE

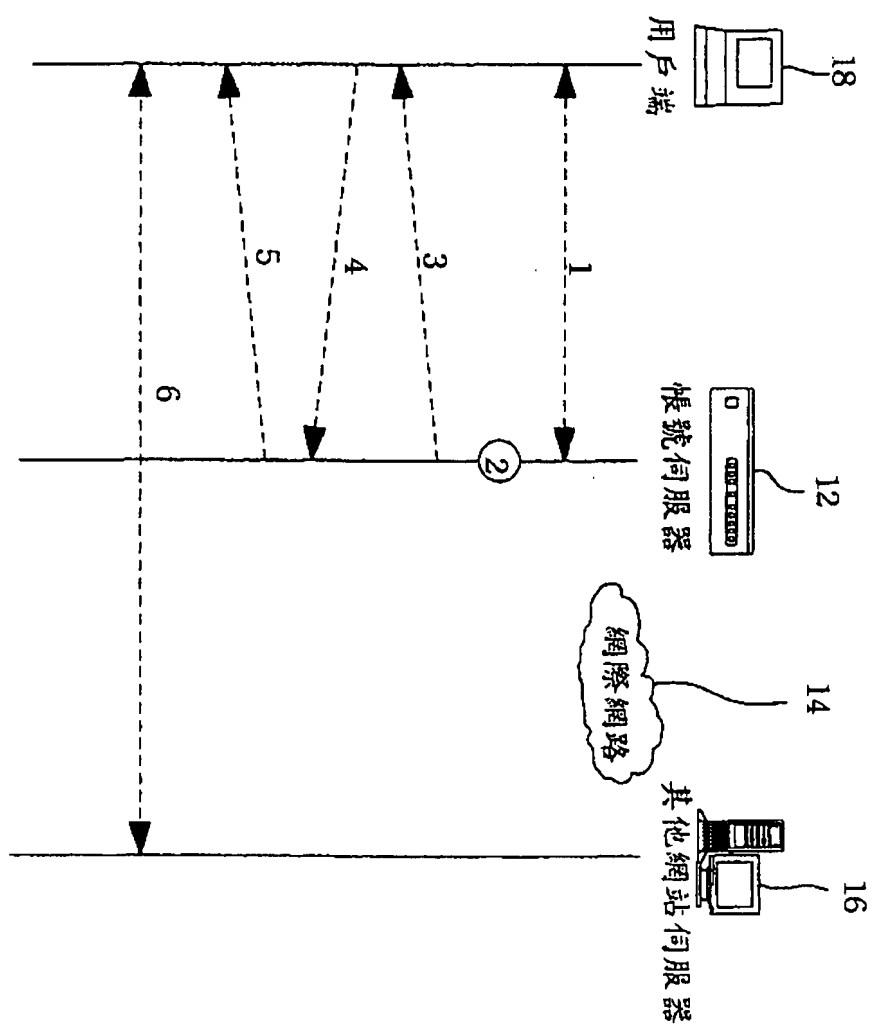


第三圖

THE



第四圖



第五圖